(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 108390878 A
(43)申请公布日 2018.08.10

(21)申请号 201810159698.X

(22)申请日 2018.02.26

(71)申请人 腾讯科技(深圳)有限公司
地址 518000 广东省深圳市南山区高新区科技中一路腾讯大厦35层

(72)发明人 叶高艺

(74)专利代理机构 深圳市隆天联鼎知识产权代理有限公司 44232
代理人 刘抗美

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 9/32(2006.01)

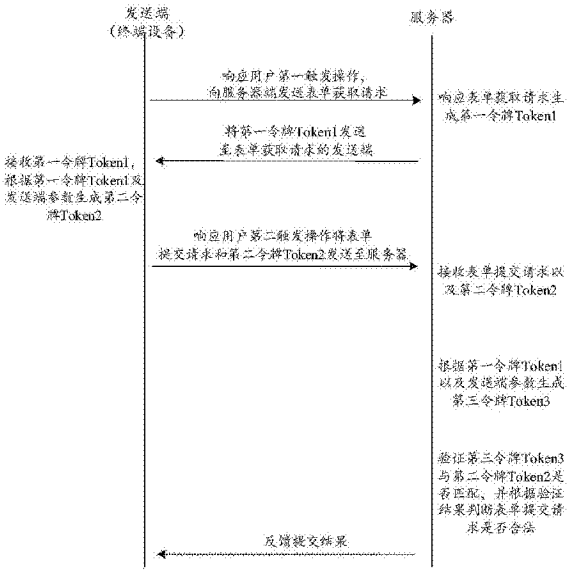
权利要求书2页 说明书12页 附图10页

(54)发明名称

用于验证网络请求安全性的方法、装置

(57)摘要

本发明涉及网络技术领域，提供了一种用于验证网络请求安全性的方法、装置、计算机可读介质及电子设备，该用于验证网络请求安全性的方法包括：响应第一网络请求生成第一令牌，并将所述第一令牌发送至所述第一网络请求的发送端；接收第二网络请求以及第二令牌；生成第三令牌；当所述第三令牌与所述第二令牌匹配时，确认所述第二网络请求合法。本发明提高了用户请求路径的安全性、保证了请求数据的有效性。



CN 108390878 A

1.一种用于验证网络请求安全性的方法，其特征在于，包括：

响应第一网络请求生成第一令牌，并将所述第一令牌发送至所述第一网络请求的发送端；

接收第二网络请求以及第二令牌；

生成第三令牌；

当所述第三令牌与所述第二令牌匹配时，确认所述第二网络请求合法。

2.根据权利要求1所述的用于验证网络请求安全性的方法，其特征在于，响应第一网络请求生成第一令牌包括：

判断所述第一网络请求是否合法；

当所述第一网络请求合法时，生成所述第一令牌。

3.根据权利要求1所述的用于验证网络请求安全性的方法，所述生成第三令牌包括：

利用所述第二网络请求的至少部分数据和/或至少一个网络参数以及所述第一令牌通过加密算法生成所述第三令牌。

4.根据权利要求1所述的用于验证网络请求安全性的方法，其特征在于，所述方法还包括：

根据所述发送端的用户标识、所述发送端的用户状态、网络请求提交时间间隔、网络请求提交次数、网络请求提交频率、所述发送端的HTTP请求头信息、所述发送端的IP地址中的一个或多个，验证所述网络数据获取请求是否合法。

5.根据权利要求1所述的用于验证网络请求安全性的方法，其特征在于，所述方法还包括：

接收第四令牌；

当所述第四令牌与所述第一令牌匹配时，确认所述第二网络请求合法。

6.根据权利要求1-5任一项所述的用于验证网络请求安全性的方法，其特征在于，所述网络请求为表单请求，所述第一网络请求为表单获取请求，所述第二网络请求为表单提交请求。

7.一种用于验证网络请求安全性的装置，其特征在于，包括：

第一令牌生成模块，用于响应第一网络请求生成第一令牌，并将所述第一令牌发送至所述第一网络请求的发送端；

信息接收模块，用于接收第二网络请求以及第二令牌；

第三令牌生成模块，用于生成第三令牌；

第一匹配验证模块，当所述第三令牌与所述第二令牌匹配时，确认所述第二网络请求合法。

8.一种用于验证网络请求安全性的方法，其特征在于，包括：

向服务器端发送第一网络请求；

接收所述服务器端返回的第一令牌；

利用所述第一令牌生成第二令牌；

发送第二网络请求和所述第二令牌。

9.根据权利要求8所述的用于验证网络请求安全性的方法，其特征在于，所述利用所述第一令牌生成第二令牌包括：

利用所述第二网络请求的至少部分数据和/或至少一个网络参数、以及所述第一令牌通过加密算法生成所述第二令牌。

10.根据权利要求8所述的用于验证网络请求安全性的方法，其特征在于，所述利用所述第一令牌生成第二令牌包括：

通过应用插件、网页控件或网页小程序生成所述第二令牌。

11.根据权利要求8所述的用于验证网络请求安全性的方法，其特征在于，所述方法还包括：

发送所述第二网络请求和所述第二令牌时，提交所述第一令牌。

12.根据权利要求8-11中任一项所述的用于验证网络请求安全性的方法，其特征在于，所述网络请求为表单请求，所述第一网络请求为表单获取请求，所述第二网络请求为表单提交请求。

13.一种用于验证网络请求安全性的装置，其特征在于，包括：

第一发送模块，用于向服务器端发送第一网络请求；

第一令牌接收模块，用于接收所述服务器端生成的第一令牌；

第二令牌生成模块，用于利用所述第一令牌生成第二令牌；

第二发送模块，用于发送第二网络请求和所述第二令牌。

14.一种计算机可读介质，其上存储有计算机程序，其特征在于，所述程序被处理器执行时实现如权利要求1-6、8-12中任一项所述的用于验证网络请求安全性的方法。

15.一种电子设备，其特征在于，包括：

一个或多个处理器；

存储装置，用于存储一个或多个程序，当所述一个或多个程序被所述一个或多个处理器执行时，使得所述一个或多个处理器实现如权利要求1-6、8-12中任一项所述的用于验证网络请求安全性的方法。

用于验证网络请求安全性的方法、装置

技术领域

[0001] 本发明涉及计算机技术领域，具体而言，涉及一种用于验证网络请求安全性的方法、装置、计算机可读介质及电子设备。

背景技术

[0002] 在客户端与服务器端交互的过程中，客户端首先需要向服务器提交网络请求；当服务器接收到该网络请求后，对其进行解析，同时生成一令牌，然后将相应的数据和令牌返回给客户端；客户端向服务器提交网络请求对应的数据，同时将令牌返回给服务器；服务器对令牌进行匹配以确认客户端是否合法。但是，恶意用户会通过爬取令牌信息、使用多个用户账号或多个代理IP地址，使用脚本模拟网络数据的提交，给用户造成人身、财产等方面的损失。

[0003] 因此本领域亟需寻求一种用于验证网络请求安全性的方法及装置，以保护用户请求路径的安全性、保证请求数据的有效性，防止恶意用户用脚本绕过浏览器批量提交数据。

[0004] 需要说明的是，在上述背景技术部分公开的信息仅用于加强对本发明的背景的理解，因此可以包括不构成对本领域普通技术人员已知的现有技术的信息。

发明内容

[0005] 本发明的目的在于提供一种用于验证网络请求安全性的方法及装置，进而保护用户请求路径的安全性、保证请求数据的有效性。

[0006] 本发明的其他特性和优点将通过下面的详细描述变得显然，或部分地通过本发明的实践而习得。

[0007] 根据本发明的第一方面，提供一种用于验证网络请求安全性的方法，其特征在于，包括：响应第一网络请求生成第一令牌，并将所述第一令牌发送至所述第一网络请求的发送端；接收第二网络请求以及第二令牌；生成第三令牌；当所述第三令牌与所述第二令牌匹配时，确认所述第二网络请求合法。

[0008] 根据本发明的第二方面，提供一种用于验证网络请求安全性的装置，其特征在于，包括：第一令牌生成模块，用于响应第一网络请求生成第一令牌，并将所述第一令牌发送至所述第一网络请求的发送端；信息接收模块，用于接收第二网络请求以及第二令牌；第三令牌生成模块，用于生成第三令牌；第一匹配验证模块，用于当所述第三令牌与所述第二令牌匹配时，确认所述第二网络请求合法。

[0009] 在本发明的一些实施例中，基于前述方案，本发明的第一令牌生成模块包括：第一判断单元，用于判断所述第一网络请求是否合法；令牌生成单元，用于在所述第一网络请求合法时，生成所述第一令牌。

[0010] 在本发明的一些实施例中，基于前述方案，本发明的第三令牌生成模块包括：第三令牌生成单元，用于利用所述第二网络请求的至少部分数据和/或至少一个网络参数以及所述第一令牌通过加密算法生成所述第三令牌。

[0011] 在本发明的一些实施例中，基于前述方案，本发明的装置包括：辅助验证模块，用于根据所述发送端的用户标识、所述发送端的用户状态、网络请求提交时间间隔、网络请求提交次数、网络请求提交频率、所述发送端的HTTP请求头信息、所述发送端的IP地址中的一个或多个，验证所述第二网络请求是否合法。

[0012] 在本发明的一些实施例中，基于前述方案，本发明的装置包括：第四令牌接收模块，用于接收第四令牌；验证模块，用于在所述第四令牌与所述第一令牌匹配时，确认所述第二网络请求合法。

[0013] 在本发明的一些实施例中，基于前述方案，本发明的装置包括：所述第一网络请求为表单获取请求，所述第二网络请求为表单提交请求。

[0014] 在本发明的一些实施例中，基于前述方案，本发明的第一令牌生成模块包括：令牌生成单元，用于根据时间戳、随机数、IP地址、第一网络请求的发送时间、前次第二网络请求提交时间、验证数据中的多种生成所述第一令牌。

[0015] 根据本发明的第三方面，提供一种用于验证网络请求安全性的方法，其特征在于，包括：向服务器端发送第一网络请求；接收所述服务器端返回的第一令牌；利用第一令牌生成第二令牌；发送第二网络请求和所述第二令牌。

[0016] 根据本发明的第四方面，提供一种用于验证网络请求安全性的装置，其特征在于，包括：第一发送模块，用于向服务器端发送第一网络请求；第一令牌接收模块，用于接收所述服务器端返回的第一令牌；第二令牌生成模块，用于利用所述第一令牌生成第二令牌；第二发送模块，用于发送第二网络请求和所述第二令牌。

[0017] 在本发明的一些实施例中，基于前述方案，本发明的第二令牌生成模块包括：第一生成单元，用于利用所述第二网络请求的至少部分数据和/或至少一个网络参数、以及所述第一令牌通过加密算法生成所述第二令牌。

[0018] 在本发明的一些实施例中，基于前述方案，本发明的第二令牌生成模块包括：第二生成单元，用于通过应用插件、网页控件或网页小程序生成所述第二令牌。

[0019] 在本发明的一些实施例中，基于前述方案，本发明的装置还包括：令牌提交模块，用于在发送所述第二网络请求和所述第二令牌时，提交所述第一令牌。

[0020] 在本发明的一些实施例中，基于前述方案，本发明的装置还包括：所述第一网络请求为表单获取请求，所述第二网络请求为表单提交请求。

[0021] 根据本发明的第五方面，提供了一种计算机可读介质，其上存储有计算机程序，所述程序被处理器执行时实现如上述实施例中所述的用于验证网络请求安全性的方法。

[0022] 根据本发明的第六方面方面，提供了一种电子设备，包括：一个或多个处理器；存储装置，用于存储一个或多个程序，当所述一个或多个程序被所述一个或多个处理器执行时，使得所述一个或多个处理器实现如上述实施例中所述的用于验证网络请求安全性的方法。

[0023] 根据本示例实施例中的用于验证网络请求安全性的方法，服务器响应第一网络请求生成第一令牌，并接收发送端发送的第二网络请求及根据第一令牌生成的第二令牌，通过服务器对第二令牌进行验证以判断第二网络请求是否合法；另外发送端发送第二网络请求和第二令牌的同时也可以提交第一令牌，通过服务器对第一令牌和第二令牌进行验证以判断第二网络请求是否合法。本发明通过第一令牌和第二令牌的双层验证保护了用户请求

路径的安全性；另外，在本发明中，服务器端还可以对提交次数、提交频率、IP地址及HTTP请求头等信息进行验证，通过多重验证保证了请求数据的有效性，防止了恶意用户用脚本绕过浏览器批量提交数据。

[0024] 本发明应当理解的是，以上的一般描述和后文的细节描述仅是示例性和解释性的，并不能限制本发明。

附图说明

[0025] 此处的附图被并入说明书中并构成本说明书的一部分，示出了符合本发明的实施例，并与说明书一起用于解释本发明的原理。显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0026] 图1示出可以应用本发明实施例的用于验证网络请求安全性的方法或用于验证网络请求安全性的装置的示例性系统架构的示意图；

[0027] 图2示出了适于用来实现本发明实施例的电子设备的计算机系统的结构示意图；

[0028] 图3示出本发明一实施例中的用于验证网络请求安全性的方法流程图；

[0029] 图4示出本发明一实施例中发送端与服务器端的交互图；

[0030] 图5示出本发明一实施例中表单获取请求合法性判断示意图；

[0031] 图6示出本发明另一实施例中表单获取请求合法性判断示意图；

[0032] 图7示出本发明一实施例中表单验证方法示意图；

[0033] 图8示出本发明又一实施例中表单提交请求合法性判断示意图；

[0034] 图9示出本发明一实施例中发送端合法性判断示意图；

[0035] 图10示出本发明一实施例中表单验证方法应用示意图；

[0036] 图11示出本发明一实施例中用于验证网络请求安全性的装置的结构示意图；

[0037] 图12示出本发明一实施例中用于验证网络请求安全性的装置的结构示意图。

具体实施方式

[0038] 现在将参考附图更全面地描述示例实施方式。然而，示例实施方式能够以多种形式实施，且不应被理解为限于在此阐述的范例；相反，提供这些实施方式使得本发明将更加全面和完整，并将示例实施方式的构思全面地传达给本领域的技术人员。

[0039] 此外，所描述的特征、结构或特性可以以任何合适的方式结合在一个或更多实施例中。在下面的描述中，提供许多具体细节从而给出对本发明的实施例的充分理解。然而，本领域技术人员将意识到，可以实践本发明的技术方案而没有特定细节中的一个或更多，或者可以采用其它的方法、组元、装置、步骤等。在其它情况下，不详细示出或描述公知方法、装置、实现或者操作以避免模糊本发明的各方面。

[0040] 附图中所示的方框图仅仅是功能实体，不一定必须与物理上独立的实体相对应。即，可以采用软件形式来实现这些功能实体，或在一个或多个硬件模块或集成电路中实现这些功能实体，或在不同网络和/或处理器装置和/或微控制器装置中实现这些功能实体。

[0041] 附图中所示的流程图仅是示例性说明，不是必须包括所有的内容和操作/步骤，也不是必须按所描述的顺序执行。例如，有的操作/步骤还可以分解，而有的操作/步骤可以合

并或部分合并，因此实际执行的顺序有可能根据实际情况改变。

[0042] 图1示出了可以应用本发明实施例的用于验证网络请求安全性的方法或用于验证网络请求安全性的装置的示例性系统架构100的示意图，该网络请求可以是表单请求、扫码登录请求等等。

[0043] 如图1所示，系统架构100可以包括终端设备101，网络102和服务器103。网络102用以在终端设备101和服务器103之间提供通信链路的介质。网络102可以包括各种连接类型，例如有线、无线通信链路或者光纤电缆等等。

[0044] 应该理解，图1中的终端设备、网络和服务器的数目仅仅是示意性的。根据实现需要，可以具有任意数目的终端设备、网络和服务器。比如服务器103可以是多个服务器组成的服务器集群等。

[0045] 用户可以使用终端设备101通过网络102与服务器103交互，以接收或发送消息等。终端设备101可以是具有显示屏的各种电子设备，包括但不限于智能手机、平板电脑、便携式计算机和台式计算机等等。

[0046] 服务器103可以是提供各种服务的服务器。例如以表单请求为例，用户利用终端设备103向服务器103发送表单获取请求，服务器响应该表单获取请求生成一第一令牌并发送至终端设备101，终端设备101根据用户输入的信息完成表单填写，同时根据第一令牌生成第二令牌，然后将表单提交请求及第二令牌或表单提交请求、第一令牌及第二令牌发送至服务器103，服务器103对第一令牌和第二令牌的有效性进行验证，以确定表单提交请求是否合法。进一步的，服务器103还对终端设备103的IP地址、HTTP请求头等信息进行验证，判断终端设备103是否合法，另外服务器103还能够对表单的提交次数和/或提交频率进行统计分析，判断用户是否为合法用户，确保了用户请求路径的安全及请求数据的有效。

[0047] 图2示出了适于用来实现本发明中的实施例的电子设备的计算机系统的结构示意图。

[0048] 需要说明的是，图2示出的电子设备的计算机系统200仅是一个示例，不应对本发明实施例的功能和使用范围带来任何限制。

[0049] 如图2所示，计算机系统200包括中央处理单元(CPU)201，其可以根据存储在只读存储器(ROM)202中的程序或者从存储部分208加载到随机访问存储器(RAM)203中的程序而执行各种适当的动作和处理。在RAM 203中，还存储有系统操作所需的各种程序和数据。CPU 201、ROM 202以及RAM 203通过总线204彼此相连。输入/输出(I/O)接口205也连接至总线204。

[0050] 以下部件连接至I/O接口205：包括键盘、鼠标等的输入部分206；包括诸如阴极射线管(CRT)、液晶显示器(LCD)等以及扬声器等的输出部分207；包括硬盘等的存储部分208；以及包括诸如LAN卡、调制解调器等的网络接口卡的通信部分209。通信部分209经由诸如因特网的网络执行通信处理。驱动器210也根据需要连接至I/O接口205。可拆卸介质211，诸如磁盘、光盘、磁光盘、半导体存储器等等，根据需要安装在驱动器210上，以便于从其上读出的计算机程序根据需要被安装入存储部分208。

[0051] 特别地，根据本发明的实施例，下文参考流程图描述的过程可以被实现为计算机软件程序。例如，本发明的实施例包括一种计算机程序产品，其包括承载在计算机可读介质上的计算机程序，该计算机程序包含用于执行流程图所示的方法的程序代码。在这样的实

施例中，该计算机程序可以通过通信部分209从网络上被下载和安装，和/或从可拆卸介质211被安装。在该计算机程序被中央处理单元(CPU)201执行时，执行本申请的系统中限定的各种功能。

[0052] 需要说明的是，本发明所示的计算机可读介质可以是计算机可读信号介质或者计算机可读存储介质或者是上述两者的任意组合。计算机可读存储介质例如可以是——但不限于——电、磁、光、电磁、红外线、或半导体的系统、装置或器件，或者任意以上的组合。计算机可读存储介质的更具体的例子可以包括但不限于：具有一个或多个导线的电连接、便携式计算机磁盘、硬盘、随机访问存储器(RAM)、只读存储器(ROM)、可擦式可编程只读存储器(EPROM或闪存)、光纤、便携式紧凑磁盘只读存储器(CD-ROM)、光存储器件、磁存储器件、或者上述的任意合适的组合。在本发明中，计算机可读存储介质可以是任何包含或存储程序的有形介质，该程序可以被指令执行系统、装置或者器件使用或者与其结合使用。而在本发明中，计算机可读的信号介质可以包括在基带中或者作为载波一部分传播的数据信号，其中承载了计算机可读的程序代码。这种传播的数据信号可以采用多种形式，包括但不限于电磁信号、光信号或上述的任意合适的组合。计算机可读的信号介质还可以是计算机可读存储介质以外的任何计算机可读介质，该计算机可读介质可以发送、传播或者传输用于由指令执行系统、装置或者器件使用或者与其结合使用的程序。计算机可读介质上包含的程序代码可以用任何适当的介质传输，包括但不限于：无线、电线、光缆、RF等等，或者上述的任意合适的组合。

[0053] 附图中的流程图和框图，图示了按照本发明各种实施例的系统、方法和计算机程序产品的可能实现的体系架构、功能和操作。在这点上，流程图或框图中的每个方框可以代表一个模块、程序段、或代码的一部分，上述模块、程序段、或代码的一部分包含一个或多个用于实现规定的逻辑功能的可执行指令。也应当注意，在有些作为替换的实现中，方框中所标注的功能也可以以不同于附图中所标注的顺序发生。例如，两个接连地表示的方框实际上可以基本并行地执行，它们有时也可以按相反的顺序执行，这依所涉及的功能而定。也要注意的是，框图或流程图中的每个方框、以及框图或流程图中的方框的组合，可以用执行规定的功能或操作的专用的基于硬件的系统来实现，或者可以用专用硬件与计算机指令的组合来实现。

[0054] 描述于本发明实施例中所涉及到的单元可以通过软件的方式实现，也可以通过硬件的方式来实现，所描述的单元也可以设置在处理器中。其中，这些单元的名称在某种情况下并不构成对该单元本身的限定。

[0055] 作为另一方面，本申请还提供了一种计算机可读介质，该计算机可读介质可以是上述实施例中描述的电子设备中所包含的；也可以是单独存在，而未装配入该电子设备中。上述计算机可读介质承载有一个或者多个程序，当上述一个或者多个程序被一个该电子设备执行时，使得该电子设备实现如下述实施例中所述的方法。例如，所述的电子设备可以实现如图3-图10所示的各个步骤。

[0056] 网络请求可以是表单请求、扫码登录请求等等，在实际应用中，网络请求在交互过程中会存在数据泄露的风险，以表单请求为例，用户可以通过表单请求按钮触发客户端向服务器发送表单获取请求，服务器响应该表单获取请求，生成令牌发送给客户端；客户端生成表单后，用户可以在表单输入框中填写信息；填写完成后通过提交按钮触发客户端将表

单提交给服务器，同时将接收到的令牌发送给服务器，服务器通过验证令牌的有效性判断表单是否合法，并对表单数据进行处理，然后销毁令牌。

[0057] 但是，在上述过程中，服务器可能无法根据表单数据判断表单的填写者是否为合法的用户，因此会有恶意用户绕过表单的人工填写步骤，通过采用自动填写程序来抓取表单页面上的令牌或获得用户登录的cookie来模拟合法用户请求，使用脚本模拟表单提交，实现自动识别表单、批量注册、自动登录等，从而进行一些恶意操作。虽然服务器能够通过限制某一账号或者某个IP的提交次数，但是恶意用户可能会申请多个账号或采用多台代理IP等手段进行脚本模拟表单提交，这大大影响了网络安全。

[0058] 针对实际应用中存在的问题，在本发明一实施例中，首先提供了一种用于验证网络请求安全性的方法，以对存在的问题进行优化处理，具体参考图3所示，用于验证网络请求安全性的方法适用于前述实施例中的所述电子设备，并至少包括以下步骤，具体为：

[0059] 步骤S310：响应第一网络请求生成第一令牌Token1，并将第一令牌Token1发送至第一网络请求的发送端；

[0060] 步骤S320：接收第二网络请求以及第二令牌Token2；

[0061] 步骤S330：生成第三令牌Token3；

[0062] 步骤S340：当第三令牌Token3与第二令牌Token2匹配时，确认第二网络请求合法。

[0063] 根据本示例实施例中的用于验证网络请求安全性的方法，服务器端响应第一网络请求生成第一令牌Token1，并发送给该第一网络请求的发送端；然后接收该发送端发送的第二网络请求和第二令牌Token2，该第二令牌Token2是该发送端根据第一令牌Token1生成的，最后对第二令牌Token2进行验证以判断第二网络请求是否合法。一方面，客户端生成第二令牌，即使第一令牌被爬取，但是没有客户端生成的第二令牌就不能通过验证，保障了网络数据提交的安全性；另一方面，即使有第二令牌，通过对第二令牌进行验证判断第二网络请求是否合法，如果验证通过则确认第二网络请求合法，因此保护了用户请求路径的安全性和请求数据的有效性，防止了恶意用户用脚本绕过浏览器提交数据。

[0064] 下面，将以表单请求为例，对本示例实施例中的用于验证网络请求安全性的方法进行进一步的说明。相应地，验证网络请求安全性的方法为表单的验证方法，第一网络请求为表单获取请求，第二网络请求为表单提交请求。

[0065] 在步骤S310：响应第一网络请求生成第一令牌Token1，并将第一令牌Token1发送至第一网络请求的发送端；

[0066] 在本示例实施例中，图4示出了发送端(终端设备101)与服务器103的交互流程图，参照图4所示，在响应一表单获取请求前，表单获取请求的发送端(终端设备101)响应用户一第一触发操作，然后向服务器103发送一表单获取请求，最后服务器103响应该表单获取请求生成第一令牌Token1，并将第一令牌Token1发送至该发送端。本示例实施例中可以包含多个终端设备，如平板电脑、智能手机、便携式计算机和台式计算机等终端设备中的一种或多种，为方便理解，下文以手机终端101作为表单获取请求的发送端进行说明。

[0067] 在本示例实施例中，服务器103响应表单获取请求生成第一令牌Token1前可以对该表单获取请求是否合法进行判断，根据判断结果确定是否生成第一令牌Token1，如果该表单获取请求合法，则生成第一令牌Token1；如果该表单获取请求不合法，则向发送端返回表单获取请求错误信息。

[0068] 进一步的，手机终端101向服务器103端发送表单获取请求时，服务器103能够获取手机终端101的用户标识，服务器103可以根据手机终端101的用户标识是否与预设数据库中的用户标识匹配，判断表单获取请求是否合法；也可以根据手机终端101的用户状态是否满足预设条件，判断表单获取请求是否合法。

[0069] 由于不同的手机终端101可能搭载不同的操作系统，那么服务器103所获得的信息也相应地会有所不同。以搭载Android操作系统的手机终端101为例，当其向服务器103发送表单获取请求时，服务器103能够获取手机终端101中的Android操作系统版本号、国际移动设备识别码IMEI、移动设备识别码MEID、用户ID等信息，服务器103可以根据所获得的信息中的部分信息，如用户ID，在服务器103中的预设数据库中查询是否存在匹配的ID，如果存在，则该表单获取请求合法；如果不存在，则该表单获取请求不合法。另外，当基于Web浏览器请求表单时，服务器103能够获得一会话ID，可以根据会话ID的有效时间是否满足预设条件判断用户状态是否正常，进而确认表单获取请求是否合法。例如预设条件为10min，当会话ID的有效时间小于或等于10min时，该用户状态正常，表单获取请求合法；当会话ID的有效时间大于10min时，则用户状态不正常，表单获取请求不合法。

[0070] 在本示例实施例中，也可以同时对用户标识和用户状态进行判断，以进一步确保表单获取请求的合法性。如图5所示，在步骤S501中，服务器103接收表单获取请求；在步骤S502中，在服务器103的预设数据库中查询是否存在手机终端101的用户标识；在步骤S503中，当确认存在匹配的用户标识后，再判断手机终端101的用户状态是否满足预设条件；在步骤S504中，如果用户状态满足预设条件，则表单获取请求合法；如果用户状态不满足预设条件，则表单获取请求不合法。

[0071] 在本示例实施例中，第一令牌Token1可以是对多项参数采用加密算法形成的加密串，例如Token1＝MD5(时间戳+Key1+IP+随机数)，其中Key1是服务器端103的验证密钥，加密算法为MD5。当然本发明并不以此为限，参数还可以包括表单请求时间、前次表单提交时间、其它验证数据等等，包含的参数越多越好；加密算法还可以是RSA、DSA、Diffie-Hellman等非对称加密算法，及AES、DES等对称加密算法中的一种或多种，本领域技术人员可以根据具体需要进行选择。另外，服务器103将第一令牌Token1发送给手机终端101的同时，将第一令牌101保存在服务器103的内存中，并且将手机终端101的相关信息保存在一缓冲存储器中，比如一命名为memcache的缓冲存储器中，用于后期对第一令牌Token1和第二令牌Token2的验证。

[0072] 在步骤S320：接收第二网络请求以及第二令牌Token2；

[0073] 在本示例实施例中，如图4所示，发送端(终端设备101)接收服务器103响应该表单获取请求生成的第一令牌Token1，并可以根据第一令牌Token1生成第二令牌Token2，然后发送端(终端设备101)响应一第二触发操作将表单提交请求和第二令牌Token2发送至服务器103。

[0074] 在本示例实施例中，第二令牌Token2与第一令牌Token1的区别在于，第二令牌Token2能够标记表单的提交是从合法的浏览器提交的，因此发送端(终端设备101)可以对第一令牌Token1、发送端(终端设备101)的参数、用户部分信息进行加密生成一加密串作为第二令牌Token2，其中发送端(终端设备101)的参数可以是终端设备101的域名、设备型号、设备ID等参数，用户部分信息可以是表单中填写的用户信息(用户名、密码、身份证号码、电

话号码、邮箱等)和/或浏览器信息(浏览器版本、浏览器证书等)等,加密算法可以是对称加密算法和/或非对称加密算法,第二令牌Token2可以采用与第一令牌Token1相同的加密算法,也可以采用不同的加密算法,本领域技术人员可以根据实际需要进行选择,本发明对此不做具体限定。

[0075] 进一步的,相关技术中通常通过判断发送端(终端设备101)的请求来源地址referer、HTTP请求头的用户代理user-agent等信息以确认发送端(终端设备101)是否合法,但是这些信息可以通过程序模拟,信任度并不高,因此为了保证表单请求和提交的安全性、有效性,可以在发送端(终端设备101)响应用户一访问表单的触发操作后,采用HTML的Object控件生成第二令牌Token2,且Object控件中的加密算法为非对称加密算法或非对称加密算法与对称加密算法的组合,例如Token2=MD5(DES.encrypt(域名+Token1+用户部分信息)),通过DES中的encrypt加密算法和MD5加密两种加密算法,提高了加密复杂度,进一步提高了表单提交请求的安全性和请求数据的有效性。当然,除了Object控件之外,其他能够在网页加载的控件也可以用于生成第二令牌,在此不再赘述。

[0076] 在步骤S330:生成第三令牌Token3;

[0077] 在本示例实施例中,服务器103根据其与发送端(终端设备101)之间的协议,可以将接收到的终端设备101的域名、用户信息及保存在内存中的第一令牌Token1,采用与生成第二令牌Token2相同的加密算法生成一第三令牌Token3,例如Token3=MD5(DES.encrypt(接收到的域名,Token1,接收到的用户部分信息)),当然本发明并不以此为限。

[0078] 在步骤S340:当第三令牌Token3与第二令牌Token2匹配时,确认第二网络请求合法。

[0079] 在本示例实施例中,服务器103接收到第二令牌Token2后,需要验证第二令牌Token2是否有效,进而判断表单提交请求是否合法。可以通过将第二令牌Token2和第三令牌Token3进行匹配,如果匹配成功,则表单提交请求合法;如果匹配失败,则表单提交请求不合法。验证结束后,服务器端103可以向发送端(终端设备101)反馈用户提交结果,当然该步骤并不是本发明所必需的。

[0080] 进一步的,服务器103可以根据表单的请求时间是否在有效时间内,判断表单提交请求是否合法,如图6所示,判断流程至少包括以下步骤,具体为:

[0081] S601:服务器103接收到所述表单获取请求时,记录当前时刻为第一时刻。

[0082] 服务器103在接收到表单获取请求时,可以在生成第一令牌Token1的同时记录当前时刻为第一时刻t1。

[0083] S602:服务器103将第一令牌Token1发送给发送端(终端设备101),并在本地保存。

[0084] 服务器103响应表单获取请求生成第一令牌Token1后,将第一令牌Token1发送给发送端(终端设备101),并保存在服务器103和发送端(终端设备101)的内存中。

[0085] S603:发送端(终端设备101)根据第一令牌Token1生成第二令牌Token2,并向服务器103发送表单提交请求和第二令牌Token2。

[0086] S604:服务器接收表单提交请求和第二令牌Token2,并记录当前时刻为第二时刻t2。

[0087] S605:根据第一时刻t1和第二时刻t2计算间隔时间△t,判断间隔时间△t是否在有效时间内。

[0088] S606:将间隔时间△t与一有效时间比较,根据比较结果判断表单提交请求是否合法。

[0089] 如果间隔时间△t不超过有效时间,则表单提交请求合法;如果间隔时间△t超过有效时间,则表单提交请求不合法(参见步骤)。举例而言,设定有效时间为1h,如果△t≤1h,则表单提交请求合法;如果△t>1h,则表单提交请求不合法。

[0090] 在本示例实施例中,发送端(终端设备101)可以将第一令牌Token1返回至服务器103,也可以不返回至服务器103。同时返回第一令牌Token1和第二令牌Token2,能够通过服务器103对第一令牌Token1和第二令牌Token2的验证进一步提高表单请求路径的安全性和数据的有效性;而仅返回第二令牌Token2,能够减少传输的数据量。如果返回第一令牌Token1时,服务器103可以接收到一由发送端(终端设备101)发送的第四令牌Token4,服务器103将第四令牌Token4与存储在memcache中的第一令牌Token1进行匹配,如果匹配成功,则表单提交请求合法,验证通过,随之服务器可以删除第一令牌Token1以节省存储空间。

[0091] 在本示例实施例中,为了进一步提高用户请求路径的安全性、请求数据的有效性,服务器103还可以对表单的提交次数、提交频率、发送端的IP地址、HTTP请求头、请求来源地址referer等信息中的一个或多个进行统计、匹配,以判断表单提交请求是否合法。如图7所示,在步骤S701中,发送端(终端设备101)发送表单获取请求;在步骤S702中,判断表单获取请求是否合法,如果合法则继续步骤S703;如果不合法则跳转到步骤S704:异常退出;在步骤S703中,服务器103响应表单获取请求生成第一令牌Token1并发送给发送端(终端设备101);在步骤S705中,发送端(终端设备101)填写表单,生成第二令牌Token2,并将表单和第二令牌Token2发送给服务器103;在步骤S706中,服务器103接收发送端(终端设备101)发送的表单提交请求和第二令牌Token2,然后验证第一令牌Token1和第二令牌Token2是否有效,如果有效则继续步骤S707;如果无效则跳转到步骤S704;在步骤S707中,服务器103可以获取发送端的HTTP请求头,对该HTTP请求头是否有效进行判断,如果有效则继续步骤S708,否则跳转至步骤S709:异常退出;在步骤S708中,服务器103对发送端(终端设备101)的IP地址进行判断,根据判断结果确定发送端(终端设备101)是否合法,如果合法则继续步骤S710,否则跳转至步骤S709;在步骤S710中,服务器103获取一统计周期内发送端提交表单的提交次数,并将提交次数与一目标值比较,如果提交次数小于目标值则表单提交请求合法,继续步骤S711,否则跳转至步骤S709;在步骤S711中,服务器103可以获取一统计周期内发送端提交表单的提交频率,并将提交频率与一目标频率比较,如果提交频率小于目标频率则表单提交请求合法,执行步骤S712:反馈用户提交结果;否则跳转至步骤S709。其中,统计周期、目标值、目标频率可以根据实际情况进行设定,比如统计周期可以设定为一天,目标值可以设定为10次,目标频率可以设定为0.5次/小时,本发明对此不做具体限定。在上述验证过程中,任意一项验证不通过,服务器103即可向发送端(终端设备101)发送无效通知,并停止处理表单数据。

[0092] 进一步的,可以创建一IP黑名单,如果某个IP地址提交了很多的恶意请求,可以将该IP地址列入IP黑名单中,当服务器接收到该IP地址提交的表单请求时,则拒绝该请求,这样可以提高数据处理速度,保证用户请求的安全性。

[0093] 值得注意的是,本发明对上述验证方法的先后顺序不做具体限定,本领域技术人员可以根据实际需要对验证流程进行安排。例如如图8所示,在步骤S801中,发送端(终端设

备101)发送表单提交请求;在步骤S802中,服务器103接收到表单提交请求后,统计表单提交次数并与目标值比较,如果表单提交次数不超过目标值则继续步骤S803,否则执行步骤S804:确认表单提交请求不合法;在步骤S803中,统计提交频率并与目标频率比较,判断提交频率是否过快,如果提交频率不超过目标频率则继续步骤S805,否则执行步骤S804;在步骤S805中,验证第一令牌Token1和第二令牌Token2是否有效;如果有效则执行步骤S806:确认表单获取请求合法,否则执行步骤S804。也可以按照图9所示的流程进行验证,如图9所示,在步骤S901中,发送端(终端设备101)发送表单获取请求;在步骤S902中,发送端(终端设备101)使用HTML的Object控件生成第二令牌Token2,当然也可以用过应用插件、网页小程序或其它网页控件生成第二令牌Token2;在步骤S903中,发送端(终端设备101)发送表单提交请求和第二令牌Token2;在步骤S904中,服务器103接收表单提交请求和第二令牌Token2;在步骤S905中,判断第二令牌Token2或第一令牌Token1与第二令牌Token2是否有效;如果有效则继续步骤S906,否则执行步骤S907:确认发送端不合法;在步骤S906中,服务器103分别对请求来源地址referer、HTTP请求头进行判断,如果请求来源地址referer为本地域名、HTTP请求头有效则执行步骤S908:确认发送端(终端设备101)合法,进而确认表单获取请求和表单提交请求合法,否则执行步骤S906。

[0094] 本发明的用于验证网络请求安全性的方法中,发送端(终端设备101)可以基于服务器端103生成的第一令牌Token1和发送端(终端设备101)的参数生成第二令牌Token2,服务器端103对接收到的第二令牌Token2或第一令牌Token1与第二令牌Token2进行验证,判断网络数据提交请求是否合法,一方面通过双令牌的验证保证了用户请求路径的安全性,另一方面通过服务器端的多重验证,保证了请求数据的有效性,有效防止了恶意用户用脚本绕过浏览器批量提交数据。

[0095] 网络请求可以是表单请求、扫码登录请求等等,通过本发明的用于验证网络请求安全性的验证方法可以提高请求数据的安全性和有效性。

[0096] 以一实际应用为例,其中网络请求为表单请求,表单的验证方法可以被广泛应用到如银行系统、网银支付、在线转账、在线注册、网站登录等多个领域。以网银支付为例,如图10所示,用户在订单付款页面选择“XX银行网银支付”,并点击“提交”按钮后,浏览器自动跳转到XX银行的客户网上银行信息确认页面,用户在相应地文本框或数据框中填写对应的信息,确认提交后,服务器端103会对用户信息进行验证,如果验证通过则在浏览器端生成一密码输入框,用户填入正确密码并“确认付款”后,服务器103将银行账户与密码进行匹配,如果匹配成功则向浏览器发送一支付成功的信息,如果匹配失败则向浏览器发送一支付失败的信息。根据本发明的表单验证方法,在上述流程中,图10(a)中点击“提交”按钮即终端设备101向服务器103发送一表单获取请求;图10(b)中提交用户信息既是向服务器103发送一表单提交请求,也是向服务器103发送另一表单获取请求,在此过程中,服务器103可以向浏览器一第一令牌Token1,终端设备101根据第一令牌Token1和终端设备101的参数生成第二令牌Token2,并在确定提交时将用户信息表单和第二令牌Token2或用户信息表单、第一令牌Token1和第二令牌Token2发送给服务器,以判断该表单提交请求是否合法;图10(c)中“确认付款”即向服务器发送一表单提交请求,在该过程中,服务器103向终端设备101发送第一令牌Token1’,终端设备101根据第一令牌Token1’和终端设备101的参数生成第二令牌Token2’,并将付款表单和第二令牌Token2’或付款表单、第一令牌Token1’和第二令牌

Token2'发送给服务器103，以判断该表单提交请求是否合法，如果合法则返回“支付成功”消息提醒。在上述的支付流程中，存在两次的表单验证过程，采用本发明的表单验证方法能够提高用户请求路径的安全性和请求数据的有效性，防止了恶意用户爬取页面信息，通过脚本提交表单请求，给用户的财产安全造成威胁。

[0097] 以下介绍本发明的装置实施例，可以用于执行本发明上述的表单验证方法。对于本发明装置实施例中未披露的细节，请参照本发明上述的表单验证方法的实施例。

[0098] 图11示出了一种用于验证网络请求安全性的装置的结构示意图。参照图11所示，用于验证网络请求安全性的装置1100可以包括：第一令牌生成模块1101、信息接收模块1102、第三令牌生成模块1103、第一匹配验证模块1104。

[0099] 具体地，第一令牌生成模块1101，用于用于响应第一网络请求生成第一令牌Token1，并将所述第一令牌Token1发送至所述第一网络请求的发送端；信息接收模块1102，用于用于接收第二网络请求以及第二令牌Token2；第三令牌生成模块1103，用于生成第三令牌Token3；第一匹配验证模块1104，用于当所述第三令牌Token3与所述第二令牌Token2匹配时，确认所述第二网络请求合法。

[0100] 在本示例实施例中，第一令牌生成模块1101包括第一判断单元11011和令牌生成单元11012。

[0101] 具体地，第一判断单元11011，用于判断所述第一网络请求是否合法；令牌生成单元11012，用于所述第一网络请求合法时，生成所述第一令牌Token1。

[0102] 令牌生成单元11012可以根据时间戳、随机数、IP地址、第一网络请求的发送时间、前次第二网络请求发送时间、验证数据中的多种生成所述第一令牌Token1。当然也可以包含其它参数，本发明对此不做具体限定。

[0103] 在本示例实施例中，第一令牌生成模块1103包括：第三令牌生成单元11031，用于利用所述第二网络请求的至少部分数据和/或至少一个网络参数以及所述第一令牌Token1通过加密算法生成所述第三令牌Token3

[0104] 在本示例实施例中，用于验证网络请求安全性的装置1100还包括辅助验证模块1105，辅助验证模块1105包括用户标识查询单元11051、用户状态判断单元11052、时间间隔获取单元11053、提交次数获取单元11054、提交频率获取单元11055、请求头信息获取单元11056、IP地址获取单元11057中的一个或多个。

[0105] 具体地，用户标识查询单元11051，用于在预设数据库中查询是否存在发送端的用户标识，并根据查询结果判断网络数据获取请求是否合法；用户状态判断单元11052，用于判断发送端的用户状态是否满足预设条件，并根据判断结果判断网络数据获取请求是否合法；提交次数获取单元11054，用于获取一统计周期内发送端提交网络请求的提交次数，并将提交次数与一目标值比较，根据比较结果判断第二网络请求是否合法；提交频率获取模块11055，用于获取一统计周期内发送端提交网络请求的提交频率，并将提交频率与一目标频率比较，根据比较结果判断第二网络请求的提交是否合法；请求头信息获取单元11056，用于获取网络请求的发送端的HTTP请求头信息，并根据请求头信息判断第二网络请求是否合法；IP地址获取单元11057，用于获取网络请求的发送端的IP地址，并根据该IP地址判断第二网络请求是否合法。

[0106] 在本示例实施例中，用于验证网络请求安全性的装置1100还包括第四令牌接收模

块1106和第二匹配验证模块1107。

[0107] 具体地，第四令牌接收模块1106，用于接收第四令牌Token4；第二匹配验证模块1107，用于当第四令牌Token4与第一令牌Token1匹配时，确认第二网络请求合法。

[0108] 此外，在本示例实施例中，时间间隔获取单元11053可以包括第一时刻记录单元110531、第二时刻记录单元110532和间隔时间计算单元110533。

[0109] 具体地，第一时刻记录单元110531，用于在接收到第一网络请求时，记录当前时刻为第一时刻t1；第二时刻记录单元110532，用于在接收到第二网络请求时，记录当前时刻为第二时刻t2；间隔时间计算单元110533，用于根据第一时刻t1与第二时刻t2计算间隔时间△t，将间隔时间△t与一有效时间比较，根据比较结果判断第二网络请求是否合法。

[0110] 在本示例实施例中，还提供了一种用于验证网络请求安全性的装置。如图12所示，用于验证网络请求安全性的装置1200可以包括：第一发送模块1201，第一令牌接收模块，第二令牌生成模块1203，第二发送模块1204。

[0111] 具体地，第一发送模块1201，用于向服务器端发送第一网络请求；第一令牌接收模块1202，用于接收服务器端返回的第一令牌Token1；第二令牌生成模块1203，用于利用第一令牌Token1生成第二令牌Token2；第二发送模块1204，用于发送第二网络请求和第二令牌Token2。

[0112] 在本示例实施例中，第二令牌生成模块1203包括：第一生成单元12031，用于利用所述第二网络请求的至少部分数据和/或至少一个网络参数、以及所述第一令牌Token1通过加密算法生成所述第二令牌Token2。

[0113] 进一步的，第二令牌生成模块1203还包括：第二生成单元12032，用于通过应用插件、网页控件或网页小程序生成所述第二令牌Token2。

[0114] 在本示例实施例中，用于验证网络请求安全性的装置1200还可以包括令牌提交模块1205，用于在发送所述第二网络请求和所述第二令牌Token2时，提交所述第一令牌Token1。

[0115] 由于本发明的示例实施例的用于验证网络请求安全性的模块的各个功能模块与上述用于验证网络请求安全性的方法的示例实施例的步骤对应，因此在此不再赘述。

[0116] 应当注意，尽管在上文详细描述中提及了表单验证装置的若干模块或者单元，但是这种划分并非强制性的。实际上，根据本发明的实施方式，上文描述的两个或更多模块或者单元的特征和功能可以在一个模块或者单元中具体化。反之，上文描述的一个模块或者单元的特征和功能可以进一步划分为由多个模块或者单元来具体化。

[0117] 本领域技术人员在考虑说明书及实践这里公开的发明后，将容易想到本发明的其它实施方案。本申请旨在涵盖本发明的任何变型、用途或者适应性变化，这些变型、用途或者适应性变化遵循本发明的一般性原理并包括本发明未公开的本技术领域中的公知常识或惯用技术手段。说明书和实施例仅被视为示例性的，本发明的真正范围和精神由所附的权利要求指出。

[0118] 应当理解的是，本发明并不局限于上面已经描述并在附图中示出的精确结构，并且可以在不脱离其范围进行各种修改和改变。本发明的范围仅由所附的权利要求来限。

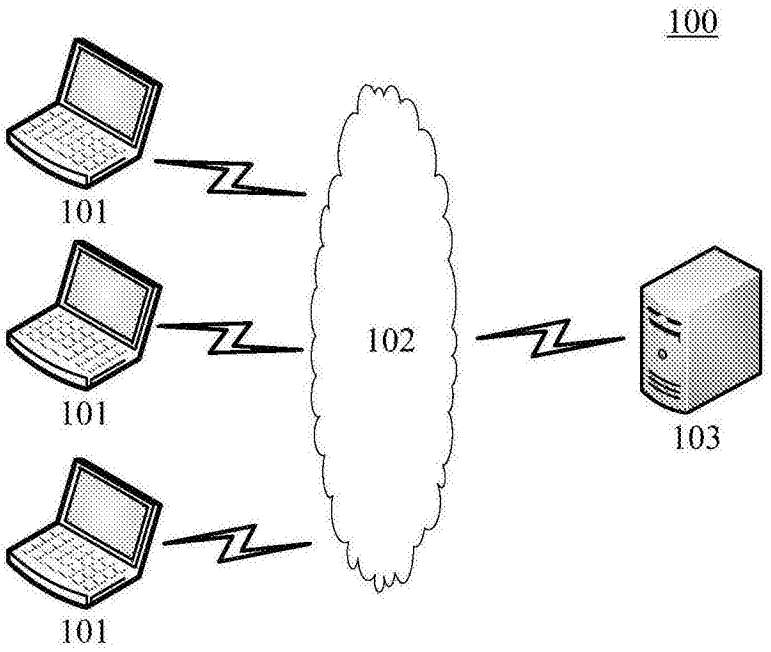

100
101
101
101
102
103

图1

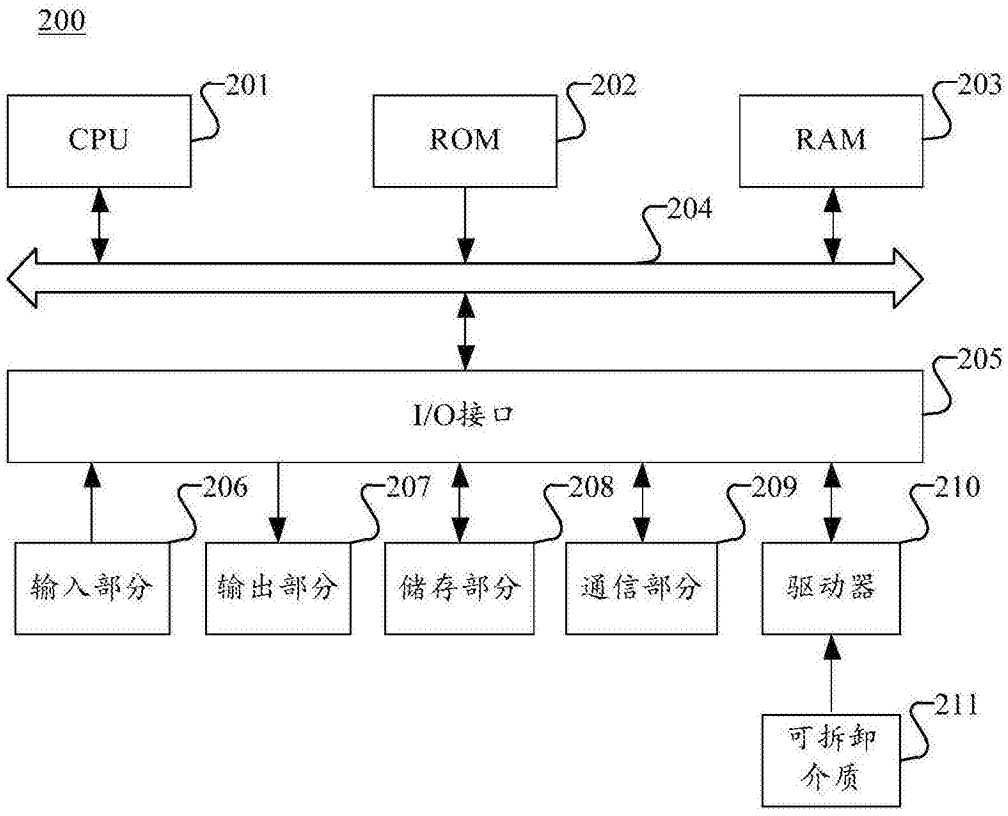

200
CPU
201
ROM
202
RAM
203
204
I/O接口
205
输入部分
206
输出部分
207
储存部分
208
通信部分
209
驱动器
210
可拆卸介质
211

图2

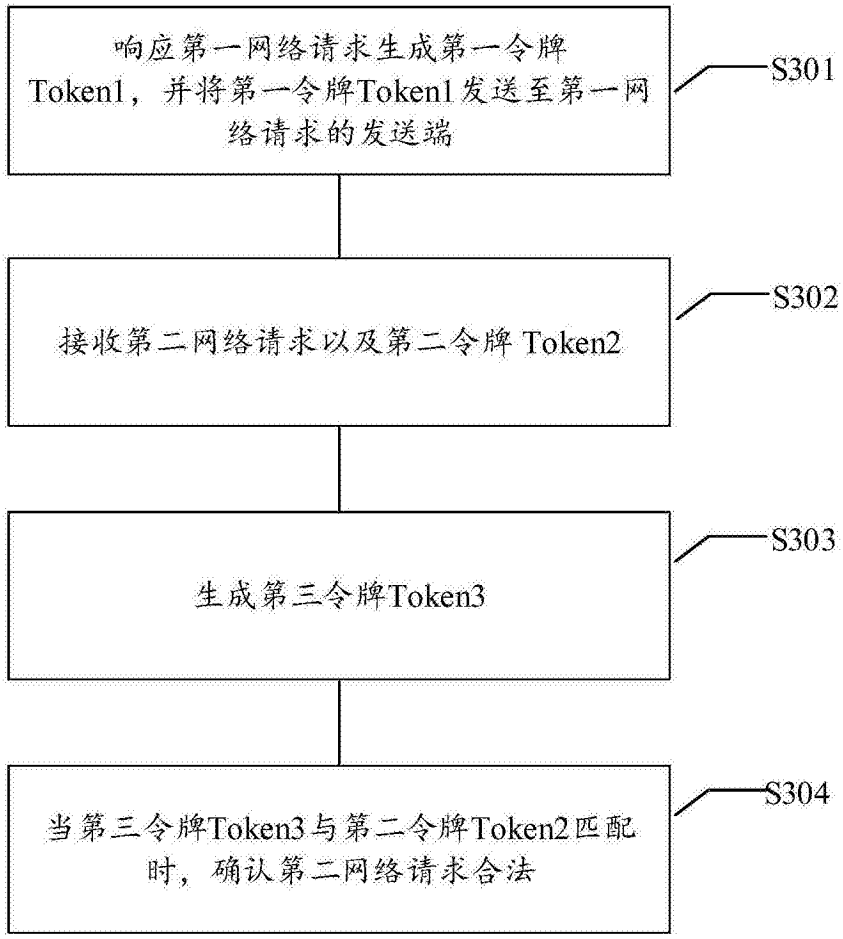

响应第一网络请求生成第一令牌Token1，并将第一令牌Token1发送至第一网络请求的发送端
S301
接收第二网络请求以及第二令牌 Token2
S302
生成第三令牌Token3
S303
当第三令牌Token3与第二令牌Token2匹配时，确认第二网络请求合法
S304

图3

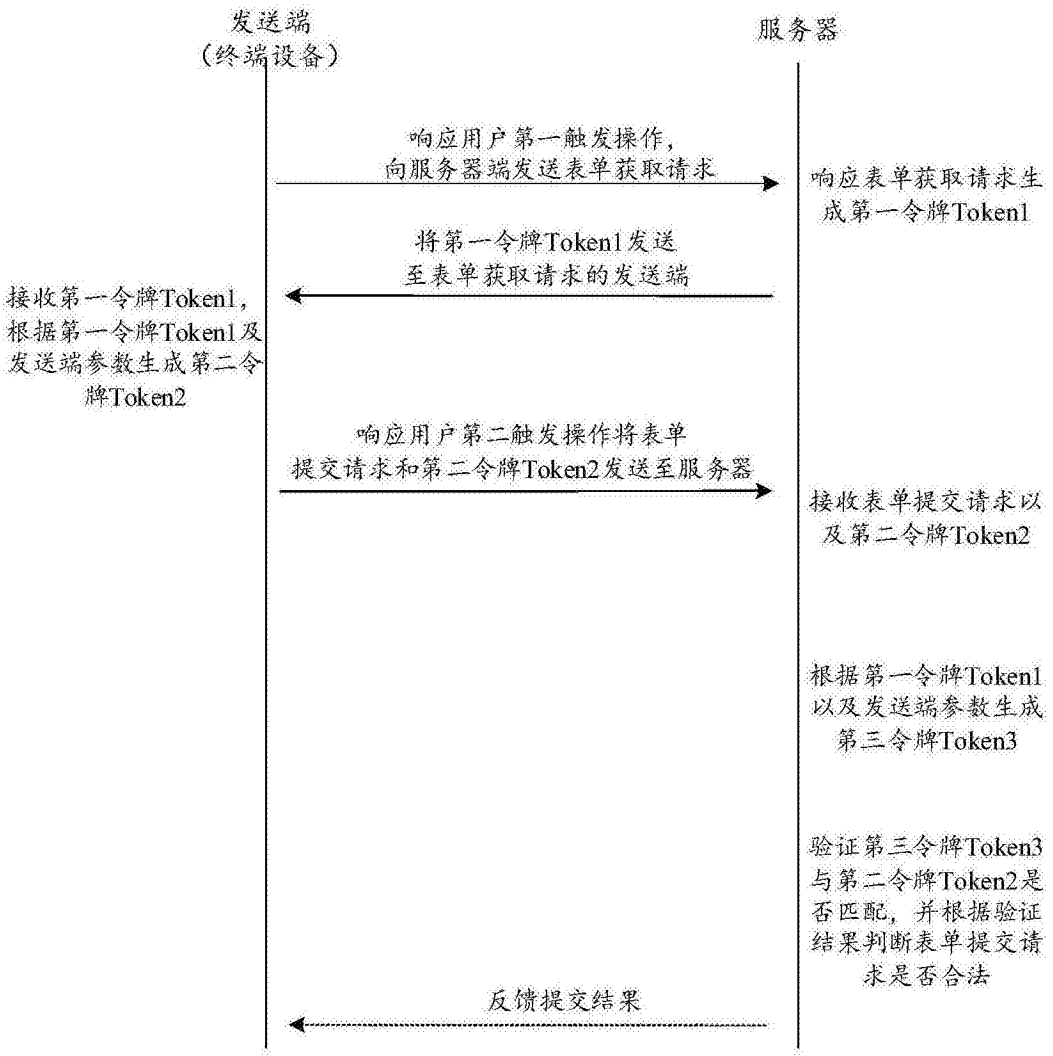

发送端
（终端设备）
服务器
响应用户第一触发操作，
向服务器端发送表单获取请求
响应表单获取请求生
成第一令牌Token1
将第一令牌Token1发送
至表单获取请求的发送端
接收第一令牌Token1，
根据第一令牌Token1及
发送端参数生成第二令
牌Token2
响应用户第二触发操作将表单
提交请求和第二令牌Token2发送至服务器
接收表单提交请求以
及第二令牌Token2
根据第一令牌Token1
以及发送端参数生成
第三令牌Token3
验证第三令牌Token3
与第二令牌Token2是
否匹配，并根据验证
结果判断表单提交请
求是否合法
反馈提交结果

图4

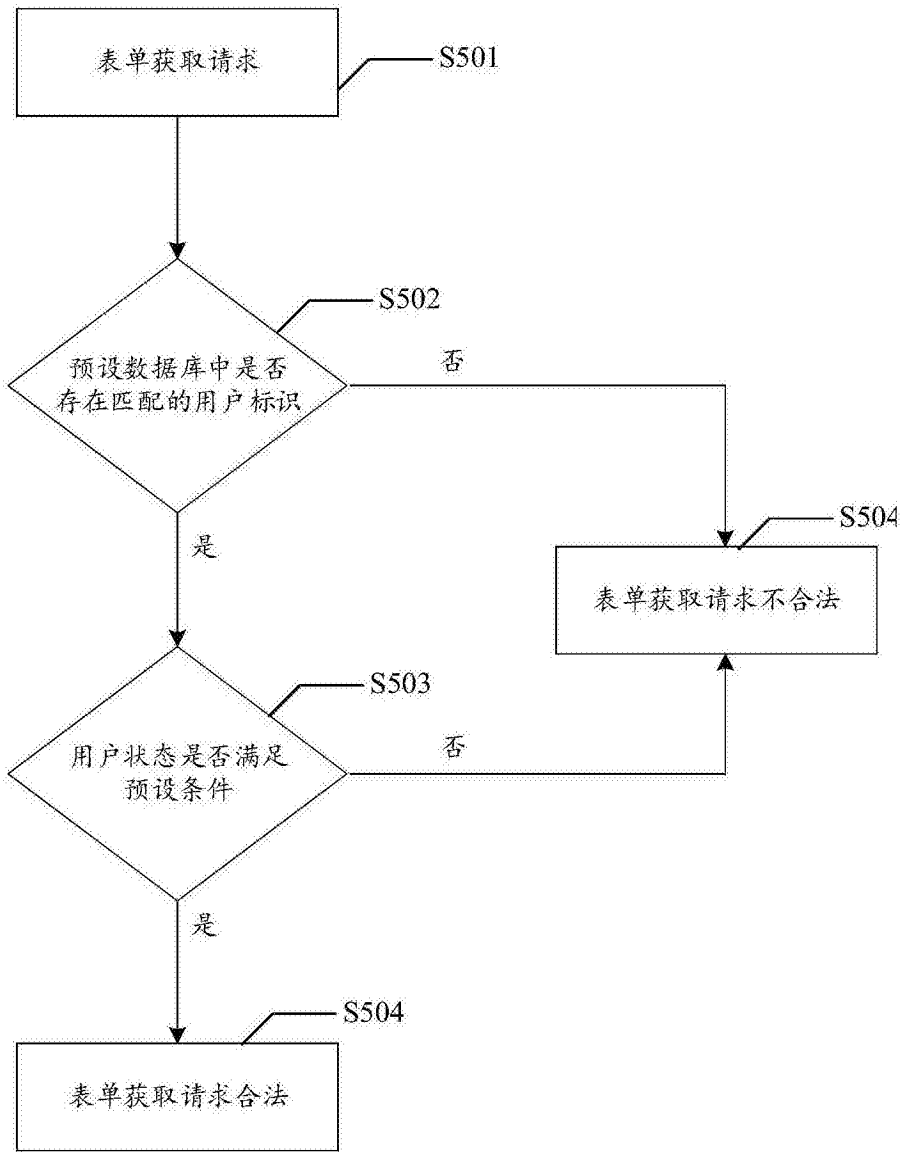

表单获取请求
S501
S502
预设数据库中是否存在匹配的用户标识
否
是
S504
表单获取请求不合法
S503
用户状态是否满足预设条件
否
是
S504
表单获取请求合法

图5

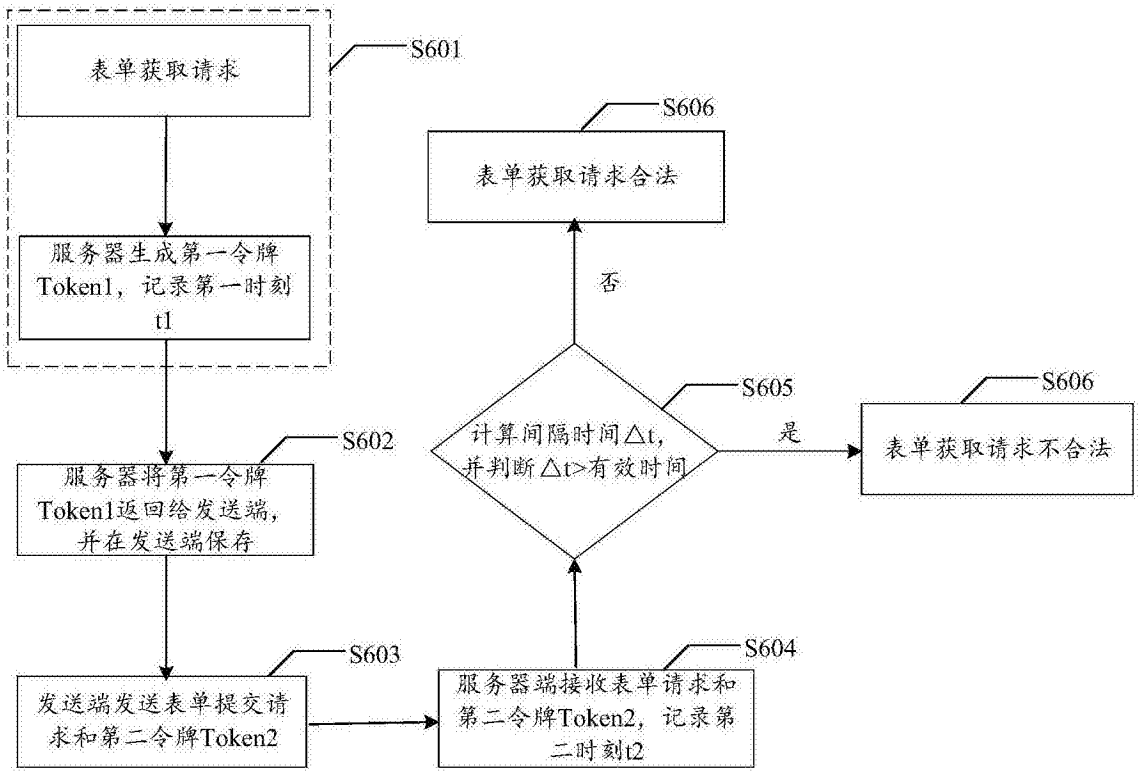

表单获取请求
S601
服务器生成第一令牌Token1，记录第一时刻t1
服务器将第一令牌Token1返回给发送端，并在发送端保存
S602
发送端发送表单提交请求和第二令牌Token2
S603
服务器端接收表单请求和第二令牌Token2，记录第二时刻t2
S604
计算间隔时间△t，并判断△t>有效时间
S605
否
表单获取请求合法
S606
是
表单获取请求不合法
S606

图6

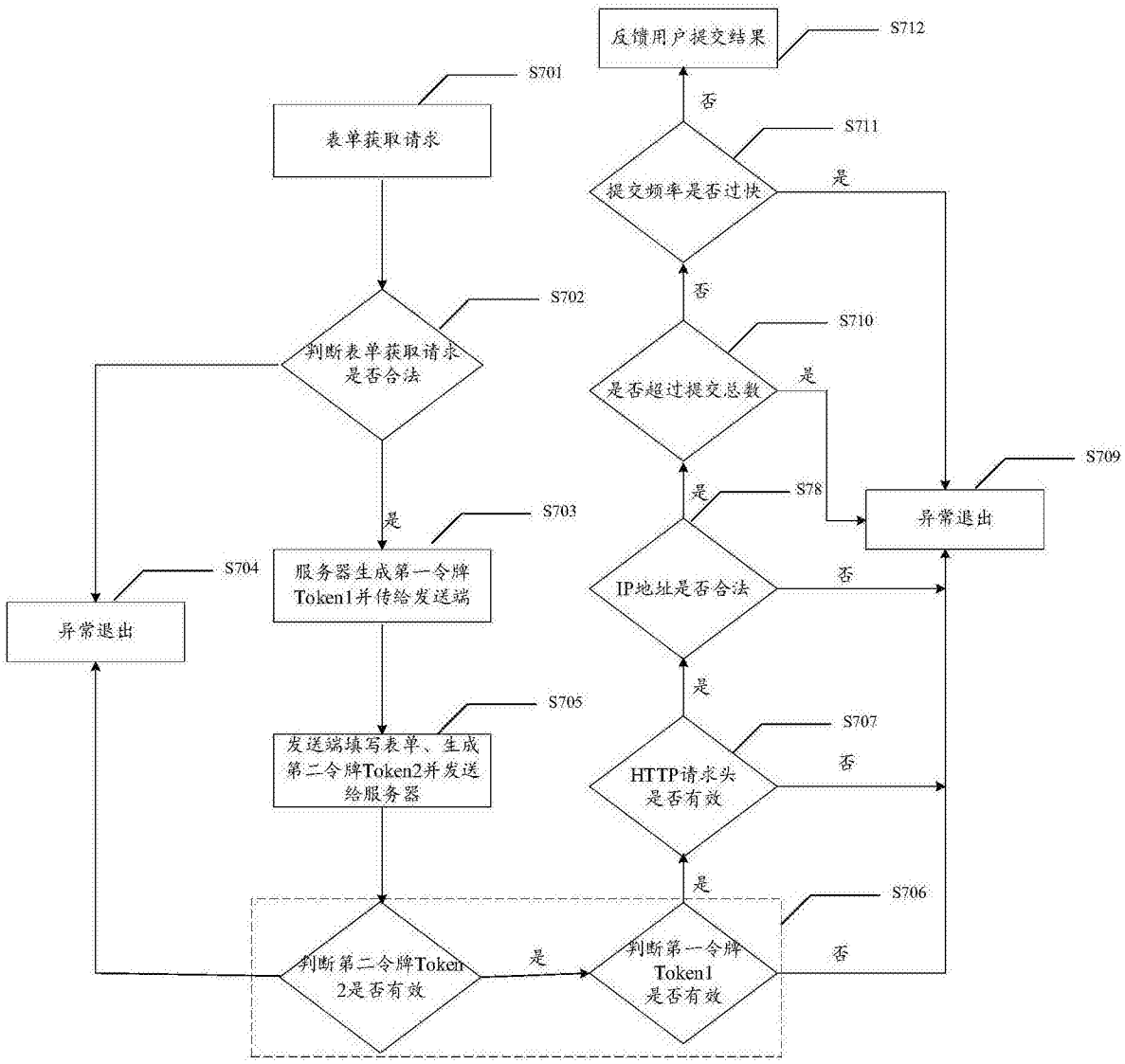

S701
表单获取请求
S702
判断表单获取请求是否合法
是
S703
服务器生成第一令牌Token1并传给发送端
否
S704
异常退出
S705
发送端填写表单、生成第二令牌Token2并发送给服务器
判断第二令牌Token2是否有效
是
判断第一令牌Token1是否有效
是
S706
否
HTTP请求头是否有效
是
S707
否
IP地址是否合法
是
S78
否
是否超过提交总数
是
S710
否
提交频率是否过快
是
S711
否
反馈用户提交结果
S712
异常退出
S709

图7

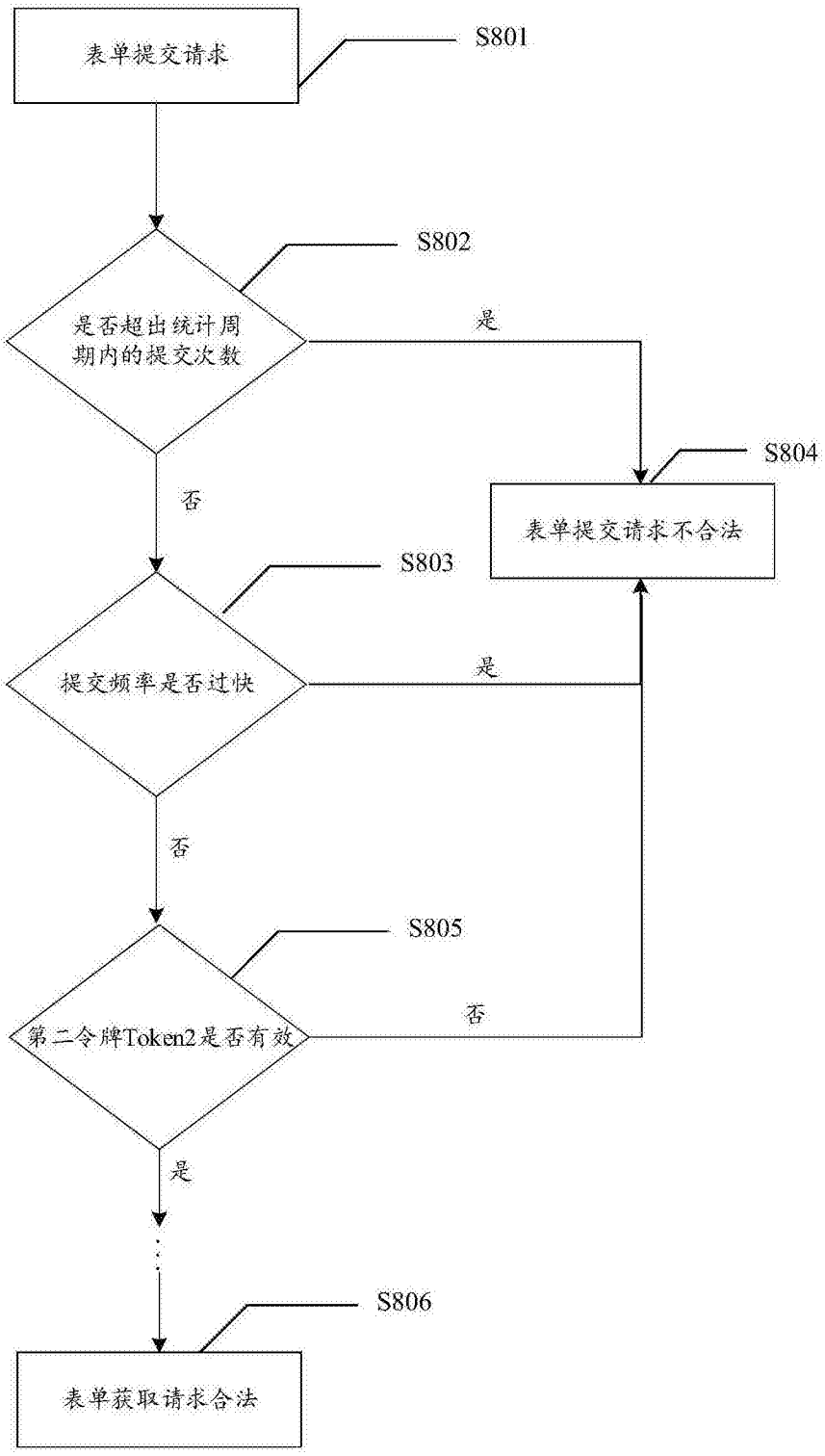

表单提交请求
S801
S802
是否超出统计周期内的提交次数
是
否
S804
表单提交请求不合法
S803
提交频率是否过快
是
否
S805
第二令牌Token2是否有效
否
是
S806
表单获取请求合法

图8

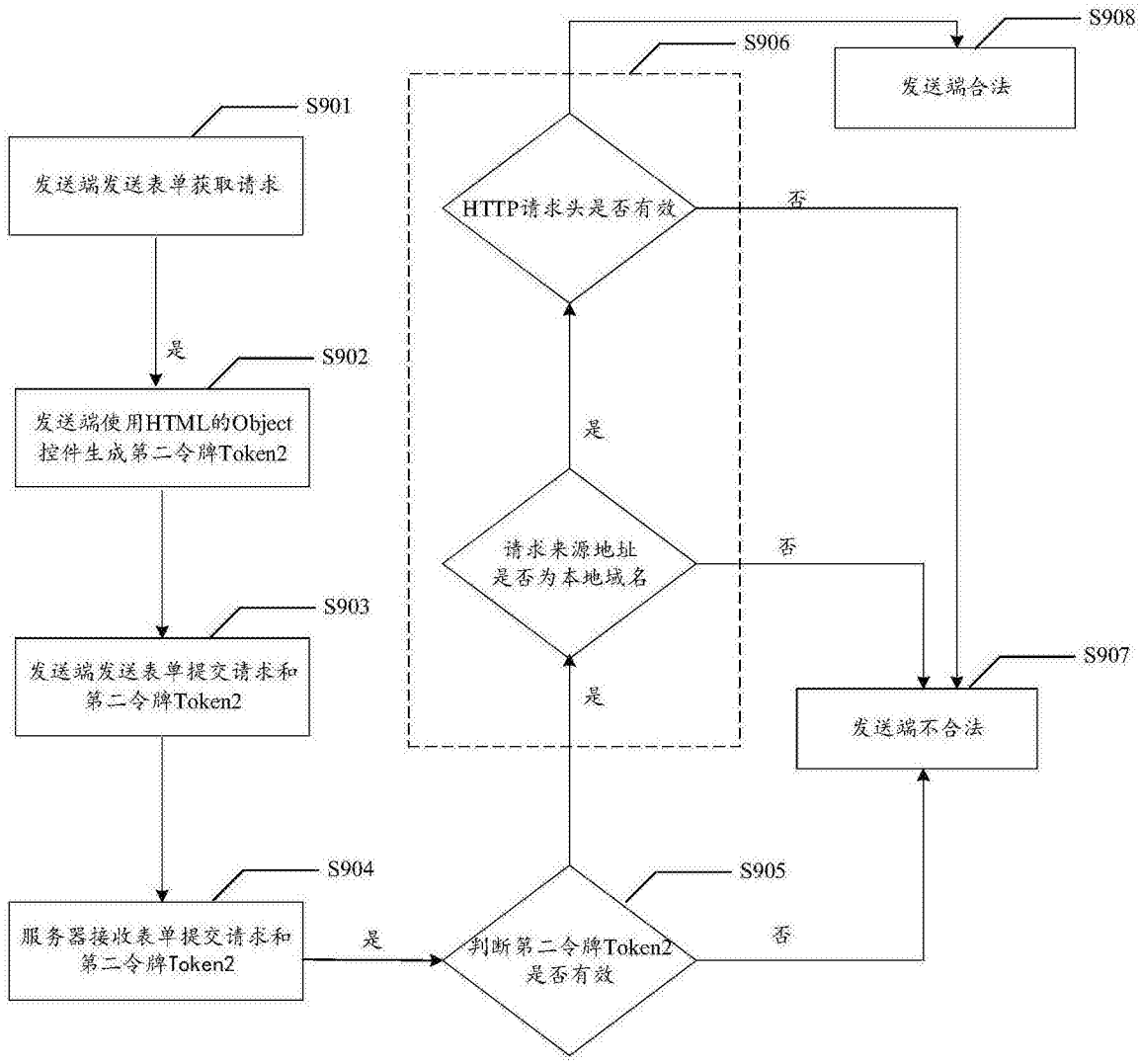
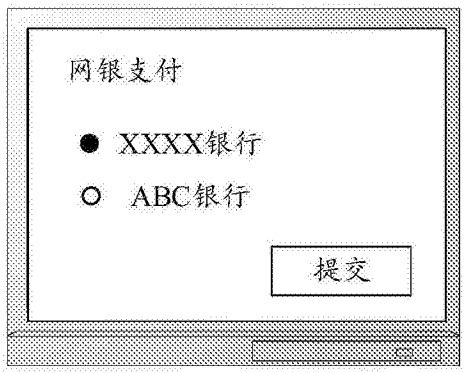
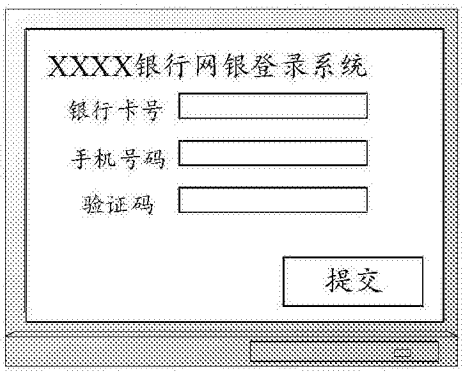

S908
S906
发送端合法
S901
发送端发送表单获取请求
HTTP请求头是否有效
否
是
S902
发送端使用HTML的Object控件生成第二令牌Token2
是
请求来源地址是否为本地域名
否
S903
发送端发送表单提交请求和第二令牌Token2
S907
是
发送端不合法
S904
S905
服务器接收表单提交请求和第二令牌Token2
是
判断第二令牌Token2是否有效
否

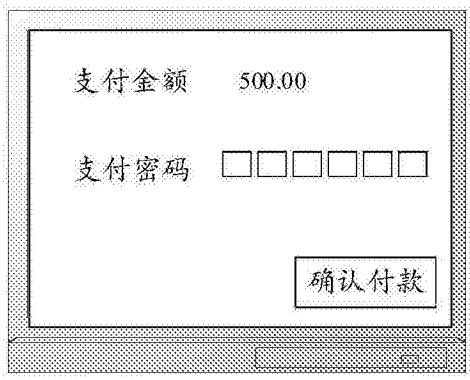
图9


网银支付
XXXX银行
ABC银行
提交

（a）


XXXX银行网银登录系统
银行卡号
手机号码
验证码
提交

（b）


支付金额 500.00
支付密码
确认付款

（c）


支付成功！

（d）

图10

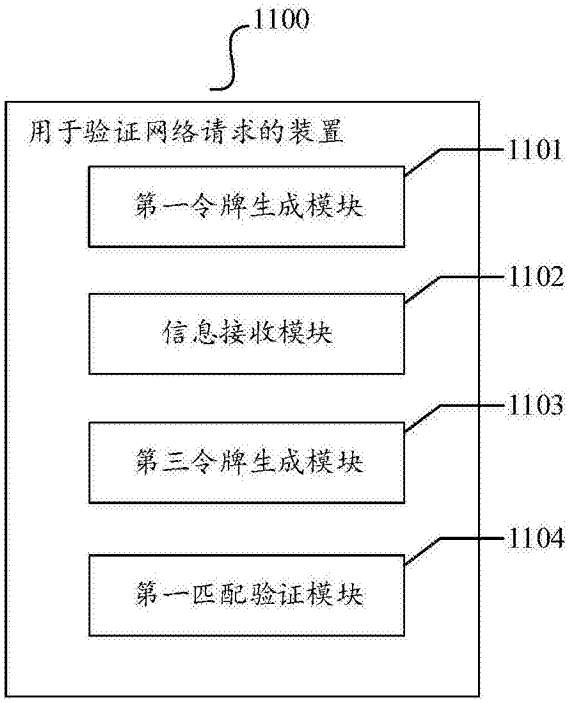

1100
用于验证网络请求的装置
1101
第一令牌生成模块
1102
信息接收模块
1103
第三令牌生成模块
1104
第一匹配验证模块

图11

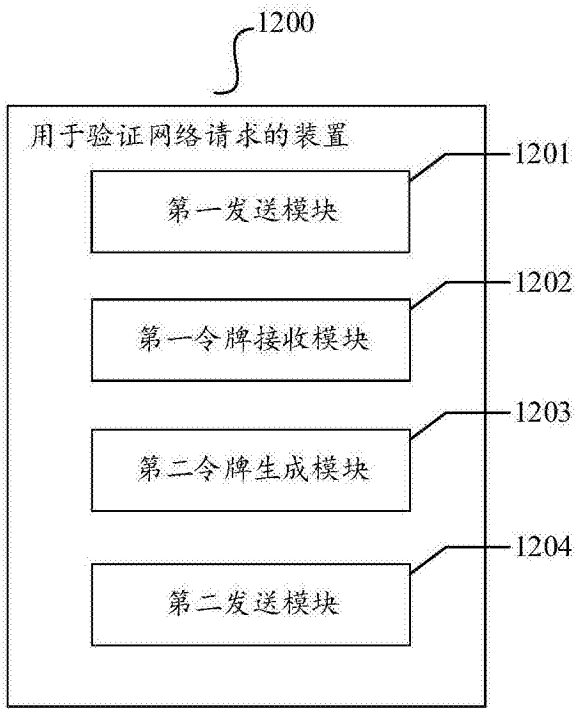

1200
用于验证网络请求的装置
1201
第一发送模块
1202
第一令牌接收模块
1203
第二令牌生成模块
1204
第二发送模块

图12